

Notice of Allowability

Application No.

09/975,302

Applicant(s)

HYPPONEN, ARI

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 1/6/2005.
2. ☒ The allowed claim(s) is/are 1-8.
3. ☒ The drawings filed on 12 October 2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

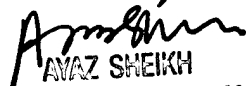
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 03032005.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Rustan J. Hill, Reg. No. 37,351 on 3/7/2005.

1. Replace claims 1,6 and 8 with:

1. A method of securing data stored on an electronic device, the method comprising:
encrypting the data using a cryptographic key
derivable from or
accessed using a passphrase;
requiring the entry into the device of the passphrase when a user wishes to access the data;
subsequently inhibiting access to the data whilst the device remains
active and
powered up; and
requiring the entry by the user into the device of a predefined password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase,
wherein, if the user fails to enter the correct password within a predefined number of attempts, the cryptographic key store by the device is

Art Unit: 2136

deleted or

re-encrypted.

6. Apparatus for securing electronic data, the apparatus comprising:

a memory for storing encrypted and unencrypted data;

first processing means for encrypting data using a cryptographic key

derivable from or

accessed using a passphrase;

input means for receiving the passphrase from a user when the user wishes to

access the data; and

second processing means for subsequently inhibiting access to the data whilst the

device

remains

active and

powered up,

for requiring the entry into the device by the user of a predefined password via

said input means when a user wishes to access the data, the password being different

from the passphrase, and

for causing the cryptographic key stored by the device to be

deleted or

re-encrypted if the user fails to enter the correct password within a

predefined number of attempts.

8. A computer storage medium having stored thereon a program for causing a computer device to secure data stored on the electronic device by:

- encrypting the data using a cryptographic key
 - derivable from or
 - accessed using a passphrase,
- requiring the entry into the device of the passphrase when a user wishes to access the data,
- subsequently inhibiting access to the data whilst the device
 - remains
 - active and
 - powered up, and
 - requiring the entry by the user into the device of a predefined password when a user wishes to access the data, the password being different from the passphrase, and,
 - in the event that the user fails to enter the correct password within a predefined number of attempts,
 - deleting or
 - re-encrypting the cryptographic key stored by the device.

Examiner's Statement of Reasons for Allowance

2. Claims 1-8 are allowed over prior art.

Art Unit: 2136

3. This action is in reply to applicant's correspondence of 06 January 2005.
4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
5. As per claims 1,6 and 8, prior art of record, Blakley, III et al, U.S. Patent 5,677,952, fails to teach, alone, or in combination, of;

(Claim 1) "A method of securing data stored on an electronic device, the method comprising:

encrypting the data using a cryptographic key

derivable from or

accessed using a passphrase;

requiring the entry into the device of the passphrase when a user wishes to access the data;

subsequently inhibiting access to the data whilst the device remains

active and

powered up; and

requiring the entry by the user into the device of a predefined password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase,

wherein, if the user fails to enter the correct password within a predefined number of attempts, the cryptographic key store by the device is

deleted or

re-encrypted.”

6. The *italicized* above claim elements dealing with (for example; claim 1) “ ... *securing data stored ... device ... encrypting ... using ... key passphrase ... entry ... passphrase when a user wishes to access the data; ... inhibiting access to the data whilst the device remains active and powered ... requiring the entry ... password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase, ... fails to enter ... password ... key store by the device is ... deleted or re-encrypted.* ” serving to patently distinguish the invention from prior art. Specifically, while the use of password and passphrase multi level security of information/data in a serially applied manner is known in the prior art (i.e., see “Mobile Computing Device Data Security Sub-Team Summary Report”, 23 July 2002, entire document, www.census.gov/procur/www/fdca/library/mcd/7-29%20MCD_WG_Security_subteam_report.pdf), the use of a part or portion of a passphrase to *first inhibit access* prior to entry of a second password, is patently distinct in the art. More specifically, the passphrase is effectively used to *enable* the password functionality only after the passphrase has been used for the cryptographic obfuscation (i.e., encryption). Further, the passphrase enablement of the subsequently entered password allows for the control of the cryptographic obfuscation function upon password entry failure (either incorrectly entered one or multiple times) via encryption key deletion, or, encryption/re-encryption.

As per the applicants arguments in the previous remarks in the Amendment (January 06 2005), the examiner finds the applicant’s arguments to be persuasive in that the art of record (Blakley, III et al) does not teach or suggest the use of multi-level security per se, let alone a

Art Unit: 2136

serial process including an inhibition of access step pending a unique password (distinct from the passphrase) entry and key deletion/encryption/re-encryption upon 1st level security user input failure (i.e., passphrase entry), so as to patently distinguish the invention from the prior art of record.

However, the claim language clearly associates the applicant's invention to inhibition of the device stored data access in an *electronic device powered up and active* per se (i.e., an electronic circuit PCB or smart card), and further that the password failure causes cryptographic key deletion or re-encryption versus the re-obfuscation of the stored data. This is in contrast to passive storage environments and technologies in general (i.e., data stored on a CD, DVD, removable media, etc.).

7. Dependent claims 2-4 and 7 are allowable by virtue of their dependencies.

Conclusion

8. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Application/Control Number: 09/975,302

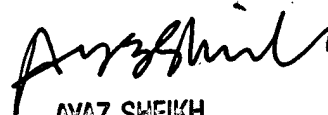
Page 8

Art Unit: 2136

Ronald Baum



Patent Examiner



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100